STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)

Section:	06	Title:	Information Security
Sub Section:	01	Title:	General Policy
Document:	03	Title:	Information Confidentiality

1. STANDARD

All information under stewardship by ISD, or on which ISD acts as a custodian, must be protected from disclosure to third parties. Third parties may be given access to information only when a demonstrable need-to-know exists, and when such a disclosure has been authorized by the State or the appointed Steward.

1.1. Summary of Standard Changes

1.2. Purpose

The protection of sensitive information concerning state employees, customers, and business transactions is of great importance. ISD Security must see that confidential information in any of these areas is not disseminated without proper authorization.

1.3. Scope

Applies to all ISD employees, customers, and public entities in their relationship to the information in which ISD acts as Steward, or for which they are custodians.

1.4. Responsibilities

1.5. Definitions and Abbreviations

1.6. Description of Standard

ISD Security will, by various means, control the flow of information to only those authorized to receive it. This will be accomplished by policy and procedures along with employee education all supporting due diligence.

1.7. Implications

Information must be classified as to the level of confidentiality.

Stewardship or custodial position, along with access restrictions and or requirements must be established and disseminated to affected personnel.

Proper security awareness must be taught and practiced by all employees.

Secondary dissemination by those approved for access of confidential information will not be allowed.

1.8. References

1.9. Attachments

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)

Section:	06	Title:	Information Security
Sub Section:	01	Title:	General Policy
Document:	03	Title:	Information Confidentiality

2.   ASSIGNMENT OF LEVEL OF CONFIDENTIALITY PROCEDURES

When an agency, through appointment as an information steward, becomes a customer of ISD they will execute a 'Information Sharing Agreement' indicating the classification of the information and who has access to it. Changes to classification or access will there after be sent directly to ISD Security by the Steward or their agent.

2.1.   Summary of Procedure Changes

1/23/02 – Revision 001 – 2.3. Added reference to document 06_01_02.doc to view copies of attachments.

2.2.   Procedure Details

2.2.1. An Information Sharing Agreement will be executed between the information steward and ISD prior to ISD becoming custodians for that information.

2.2.2. Any changes, additions, deletions to access permissions or information classification will be given to ISD through a properly excited Access Request Form.

2.3.   References

Data Sharing Agreement (See 6.1.2 'Attachments')
Access Request Form

2.4.   Attachments

3.   INTERNAL CONFIDENTIALITY PROCEDURES

Employees will not allow confidential information to be disseminated through negligence.

3.1.   Summary of Procedure Changes

3.2.   Procedure Details

3.2.1. ISD employees will not divulge the nature (data dictionary, etc.) or location of information.

3.2.2. All confidential information in the workplace will be secured when the employee is not present including lockup, clean workspaces, and secured workstations.

3.2.3. Delivery of hard copy confidential information will be person-to-person with transporting vehicles secured at all times.

3.2.4. Unauthorized browsing of system's of network information is restricted to job specific tasks.

Section:	06	Title:	Information Security
Sub Section:	01	Title:	General Policy
Document:	03	Title:	Information Confidentiality

3.3.   References

3.4.   Attachments

4.   INFORMATION DISPOSAL PROCEDURES

4.1.   Summary of Procedure Changes

4.2.   Procedure Details

Refer to Section 6 (ISD Security), Sub-Section 3 (Information Security), Document 5 (Information Storage, Back-up, Disposal) for procedural details.

4.3.   References

4.4.   Attachments